NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPROVEMENT OF THE DHRA-DMDC PHYSICAL ACCESS SOFTWARE DBIDS USING CLOUD COMPUTING TECHNOLOGY: A CASE STUDY

by

Duy T. Luc

June 2012

Thesis Co-Advisors: Man-Tak Shing
James Bret Michael

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2012	Master's Thesis

4. TITLE AND SUBTITLE Improvement of DHRA-DMDC Physical Access Software DBIDS Using Cloud Computing Technology: A Case Study	5. FUNDING NUMBERS
6. AUTHOR(S) Duy T. Luc	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number: N/A.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200words)

The U.S government has created and been executing an Identity and Management (IdM) vision to support a global, robust, trusted and interoperable identity management capability that provides the ability to correctly identify individuals and non-person entities in support of DoD mission operations. Many Directives and Instructions have been issued to standardize the process to design, re-designed new and old systems with latest available technologies to meet the vision's requirements. In this thesis we introduce a cloud-based architecture for the Defense Biometric Identification System (DBIDS), along with a set of DBIDS Cloud Services that supports the proposed architecture. This cloud-based architecture will move DBIDS in the right direction to meet Dod IdM visions and goals by decoupling current DBIDS functions into DBIDS core services to create interoperability and flexibility to expand future DBIDS with new requirements.

The thesis will show its readers how DBIDS Cloud Services will help Defense Manpower Data Center (DMDC) easily expanding DBIDS functionalities such as connecting to other DMDC services or federated services for vetting purposes. This thesis will also serve as a recommendation of a blue-print for DBIDS architecture to support new generation of DBIDS application. This is a step closer in moving DMDC Identity Enterprise Solution toward DoD IdM realizing vision and goals. The thesis also includes a discussion of how to utilize virtualized DBIDS workstations to address software-deployment and maintenance issues to resolve configuration and deployment issues which have been costly problems for DMDC over the years.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Cloud Computing Technology, Virtualization, SOA, Web Services, PKI	70
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 8–98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IMPROVEMENT OF THE DHRA-DMDC PHYSICAL ACCESS SOFTWARE DBIDS USING CLOUD COMPUTING TECHNOLOGY: A CASE STUDY

Duy T. Luc
Civilian, Department of Defense
B.S, California State University, San Jose, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SOFTWARE ENGINEERING

From the

NAVAL POSTGRADUATE SCHOOL
June 2012

Author: Duy T Luc

Approved by: Man-Tak Shing
Thesis Co-Advisor

James Bret Michael
Thesis Co-Advisor

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The U.S government has created and been executing an Identity and Management (IdM) vision to support a global, robust, trusted and interoperable identity management capability that provides the ability to correctly identify individuals and non-person entities in support of DoD mission operations. Many Directives and Instructions have been issued to standardize the process to design, re-designed new and old systems with latest available technologies to meet the vision's requirements. In this thesis we introduce a cloud-based architecture for the Defense Biometric Identification System (DBIDS), along with a set of DBIDS Cloud Services that supports the proposed architecture. This cloud-based architecture will move DBIDS in the right direction to meet Dod IdM visions and goals by decoupling current DBIDS functions into DBIDS core services to create interoperability and flexibility to expand future DBIDS with new requirements.

The thesis will show its readers how DBIDS Cloud Services will help Defense Manpower Data Center (DMDC) easily expanding DBIDS functionalities such as connecting to other DMDC services or federated services for vetting purposes. This thesis will also serve as a recommendation of a blue-print for DBIDS architecture to support new generation of DBIDS application. This is a step closer in moving DMDC Identity Enterprise Solution toward DoD IdM realizing vision and goals. The thesis also includes a discussion of how to utilize virtualized DBIDS workstations to address software-deployment and maintenance issues to resolve configuration and deployment issues which have been costly problems for DMDC over the years.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. MOTIVATION 1
B. PURPOSE 1
C. ORGANIZATION 2

II. DOD IDENTITY MANAGEMENT AND DBIDS 3
A. DOD IDENTITY MANAGEMENT 3
1. Overview 3
2. Issues Regarding Identity Management (IdM) 3
3. DoD IdM Vision, Goals and Benefits 4
4. Current Approach 5
a. Non-DoD Directives 6
b. DoD Directives, Regulations and Instructions 7
B. DBIDS 8
1. Overview 8
2. Limitation of Current DBIDS Architecture 8
3. Potential DBIDS with Cloud Computing 9

III. CURRENT DBIDS DESIGN AND IMPLEMENTATION 11
A. DBIDS SOFTWARE REQUIREMENTS 11
1. Business Context 11
a. Personnel Vetting 11
b. Access Control 12
c. Identity Management 12
d. Verification 12
e. Authorization 12
2. Functional Requirements 16
a. Use Cases 16
b. Additional Features 21
3. Non-Functional Requirements 21
a. Performance Requirements 21
b. Security Requirements 22
c. Graphic User Interface (GUI) Requirements 22
B. CURRENT DBIDS SOFTWARE DESIGN AND ARCHITECTURE 22
1. Architecture Logical View 22
2. DBIDS Workstations 23
C. PROBLEMS WITH CURRENT DBIDS DESIGN 24

IV. DBIDS DESIGN WITH CLOUD COMPUTING 27
A. DBIDS CLOUD SERVICES LAYER (SAAS) 28
1. DBIDS Cloud Services 28
B. DBIDS SECURITY SERVICE LAYER 30
C. DBIDS INFRASTRUCTURE LAYER (IAAS) 30
1. Oracle Cloud File System Solution 31

2. Hibernate 31
3. Database Design 32
D. DBIDS CLOUD VIRTUALIZED APPLICATIONS 35
E. DBIDS CLOUD VIRTUALIZED WORKSTATIONS 37
1. Desktop Virtualization Technology 37
2. Virtualized Development/Testing Workstations 38
3. Centralized Virtual Deployed Workstations 39
4. DBIDS Workstation Virtualization Benefits 41
F. VENDORS VIRTUALIZED APPLICATIONS 42
V. CONCLUSION AND FUTURE RESEARCH 45
A. SUMMARY 45
B. FUTURE WORK 46
1. Cloud Security 46
2. Scaling-Up 47
3. Web-Based Services (Thin Client Layer) 48
LIST OF REFERENCES 49
INITIAL DISTRIBUTION LIST 51

LIST OF FIGURES

Figure 1. DBIDS Installation Overview 14
Figure 2. DBIDS Access Authorization Use Case 18
Figure 3. DBIDS Law Enforcement Report Use Case 20
Figure 4. DBIDS Components Logical View 23
Figure 5. DBIDS Private Cloud Architecture View 27
Figure 6. DBIDS Database Component Diagram (After DMDC-DBIDS Technical Specification) 33
Figure 7. DBIDS Virtual Applications Component Diagram 36
Figure 8. DBIDS Virtual Applications GUI Layout Component (From DMDC-DBIDS Technical Specification) 36
Figure 9. DBIDS Virtualized Workstations Diagram 39

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Person Registration Use Case (From DMDC-DBIDS Functional Specification) 17
Table 2. Access Authorization Use Case (From DMDC-DBIDS Functional Specification) 19
Table 3. Law Enforcement Report Use Case (From DMDC-DBIDS Functional Specification) 20
Table 4. Web Services Component Description 29

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFIS - Automation Fingerprint Identification System

AWS - Amazon Web Service

BFC - Biometrics Fusion Center

CPU - Central Processing Unit

CSA - Cloud Security Alliance

CIO - Chief Identity Officer

CAC - Common Access Card

CRD - Credential

DBIDS - Defense Biometrics Identification System

DoD - Department of Defense

DHRA - Defense Human Resource Activity

DMDC - Defense Manpower Data Center

DEERS - Defense Enrollment Eligibility Reporting System

FBI - Federal Bureau of Investigation

FIPS - Federal Information Processing Standards

GUI - Graphic User Interface

HSPD - Homeland Security Presidential Directive

HTTP - HyperText Transfer Protocol

IT - Information Technology

IaaS - Infrastructure as a Service

IDM - Identity Management

NIST - National Institute of Standards and Technology

NESI - Net-Centric Enterprise Solutions for Interoperability

NIPRNET - Non-classified Internet Protocol Router Network

PII - Personally Identifiable Information

PIV - Person Identity Verification

PKI - Public Key Infrastructure

PDA - Personal Digital Assistant

PaaS - Platform as a Service

REST - Representational state transfer

RA - Registration Authorization
SOA - Service Oriented Architecture
SaaS - Software as a Service
SDO - Standard Development Organization
SOAP - Simple Object Access Protocol
SIPRNET - Secret Internet Protocol Router Network
UDDI- Universal Description, Discovery and Integration
W3C - The World Wide Web Consortium
WSDL - Web Service Definition Language
WS - Web Services
WAN - Wide Area Network
XML - Extensible Markup Language
VDI - Virtual Desktop Integration

ACKNOWLEDGMENTS

I dedicate this thesis to my wife, Thanh Nguyen, and our handsome prince, Dylan, who supported me while I was working late trying to finish this project.

I would also like to thank Professors Shing and Michael for their time and patience throughout the supervision of my thesis research. I am a better software engineer today because of their guidance and outstanding mentorship.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

As stated in the 2008 National Defense Strategy,

> Intelligence and information sharing have always been a vital component of national security. Reliable information analysis, quickly available, is an enduring challenge…Concept such as "net-centricity" can help guide DoD, linking components of the Departments together and connecting organizations with complementary core competencies, forging the total Task Force into more than the sum of its part. The goal is to break down barriers and transform industrial-era organizational structure into an information and knowledge-based enterprise.

In order to meet DoD vision and goals, the Defense Manpower Data Center (DMDC) organization as a whole has been realizing its 5-years plan to institutionalize Federated identity within the DoD, to be the central repository for the identity management with real-time authentication and authorization solution, providing current and consistent person and personnel data for both the classified and non-classified environments. As part of DMDC, the Identity Division has set its mission to ensure that the right people, and only the right people, have the right access, at the right time, to defend and protect the personnel, logical and physical assets of the Department.

B. PURPOSE

This thesis addresses the following questions:

1. How can DoD leverage cloud computing to enhance the existing Defense Biometrics Identification System (DBIDS) software to be compatible with HSDP-12 Directive and aligned DoD IdM vision.
2. How can a DBIDS cloud platform permit multiple vendors to create and develop applications to enhance physical-access-control solutions?

DBIDS is a government-owned application. It is developed and deployed by the DMDC as a force-protection program to manage personnel and installation access at DoD facilities. The DBIDS software application allows operators to register personnel data into a database, capture biometric information, and retrieve that data and biometric information for verifying and validating (V&V) the identity of individuals attempting to gain access to military installations. The software supports the adding, retrieving, updating, and displaying of such information. Currently, support for maintaining and upgrading the BIDS software, servers and devices, for expanded features and bug fixes is manpower-intensive. In this thesis, we investigate how DMDC can leverage cloud computing to support the DoD IdM vision and goals and to lower its total cost of ownership of DBIDS.

C. ORGANIZATION

Chapter II contains an overview DoD Identity Management (IdM), its original issues, and current state of DoD IdM vision, goals and benefits. Chapter III describes the existing architecture of DBIDS, some of the significant limitations of the current DBIDS design, and some of the problems that DBIDS owners and users experienced in the operation of the Physical Access Control System (PACS). Chapter IV presents the analysis and the evaluation of the new DBIDS's software architecture, which utilizes cloud computing technology and SOA design principles. It also presents solutions for problems in legacy DBIDS versions. Chapter V contains a summary of the research and recommendations for future work.

II. DOD IDENTITY MANAGEMENT AND DBIDS

A. DOD IDENTITY MANAGEMENT

1. Overview

Since 2007, DoD had launched a proposed vision for achieving effective information sharing across internal and external agencies required to ensure mission success. DoD has been carried out this vision through implementation of the DoD Net-Centric Data and Net-Centric Services Strategies. Within these strategies, the DoD Information Sharing Implementation Plan addresses management, operations, classification and marking processes, identity and access management, technical infrastructure, and federal government wide information sharing initiatives (The Office of Assistant Secretary of Defense, “Network and Information Integration” Report, 2009).

DoD Identity and Access Management is the combination of the policy, processes and technology used to authoritatively establish and manage personnel identities represented in DoD. Software tools are created to implement rules and procedures that defines an agreement between an individual and an organization regarding ownership, and safeguard of personal identity information. These tools are used to validate DoD affiliation, authorize credential holder and establish a trustworthy process for assigning attributes to a digital identity and to connect that identity to an individual.

2. Issues Regarding Identity Management (IdM)

Today, the United Sates constantly faces the security challenges to protect digital information and communication infrastructure. The need for information sharing has pushed the government to do more to address these threats. Currently, there exist many IdM systems from different agencies across the entire government that were developed to address IdM challenges. According to “Identity Management Task Force” report on 2008, here are some of the common problems for current existing IdM systems within our government:

- Duplicative identity data is often stored in multiple locations within the same agency, as well as across agencies, causing a negative impact on accuracy and complicating an individual's attempt at redress.
- A lack of commonly used standards makes appropriate cross function collaboration difficult, thus impacting both time-sensitive mission needs as well as reducing personal privacy.
- Privacy protection efforts vary in complexity across agencies.
- There is no single government-wide forum responsible for coordinating and homogenizing IdM efforts across the U.S. government.
- Interoperability shortfalls: Discovery and domain resolution, need for greater trust, IdM systems that rely on loosely-coupled identities, lack of consistent metrics.

3. DoD IdM Vision, Goals and Benefits

DoD visions to create a federated approach IdM architecture for leveraging broad-use PII (Personally Identifiable Information) elements to maximize accuracy, availability, privacy protection, and management of this data. Individual applications would access this data through a network grid, which can be established using common technical standards and policies to ensure appropriate use and control. Once verified, broad-use PII can be augmented with application specific PII in order to make operational decisions. DoD IdM goals are:

- Configuration and operation of a "network of networks" to securely manage digital identities, based on a set of common data elements for stored PII that will allow it to be leveraged by a broad range of applications.

- Security of process, data transmission, and storage; this includes and embraces all features of confidentiality, integrity, authenticity, and privacy, including use of encryption and authentication.
- Audit ability of processes, with complete, automatic, and secure record keeping.
- Information availability, at global distances, of strong verification of stored digital identity when called for or needed to support an authorized application.
- Standards-based connectivity, interoperability, and extensibility of supporting IT architecture.
- Preservation of application-specific PII data under control of application sponsors, with minimal exposure to unauthorized access or unnecessary transmission across networks.
- Ability of prospective application sponsors to develop, install, and operate applications in a way that permits the supporting IT grid to be seen as a freely available, ubiquitous service.

DoD IdM benefits are:

- Enhanced accuracy and management of PII that is used by multiple applications.
- Clear separation of application-specific PII and tighter controls to ensure this information is not shared across domains.
- A uniform, more transparent approach of handling PII.
- Minimizations of duplicative efforts to generate, maintain, and safeguard PII.
- Providing the government a better understanding of and ability to macro-manage its IdM activities.

4. Current Approach

U.S. government and DoD need a common, interoperable, integrated policies, processes and technology to identify, verify and authorize human

identities. These processes should support real-time authentication and authorization to fulfill the requirement of DoD Net-Centric service vision. There is a need for authoritative central data source for personal information, biometric information, law enforcement information (security alert information). There should be a central source for continuous personnel background investigation, adjudication, and clearance.

a. Non-DoD Directives

HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors was issued by the President in August 2004. According to the Directive:

> Wide variations in the quality and security of forms of identification used to gain access to secure federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase government efficiency, reduces identity fraud, and protects personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees).

The Department of Commerce has been tasked to design a federal ID standard. In February 2005, the Department of Commerce released the Federal Identity Standard through the National Institute of Standards and Technology as the Federal Information Processing Standard Publication201 (FIPS-201).

FIPS-201: "Personal Identity Verification (PIV) of Federal Employees and Contractors," February 25, 2005, provides standards for the identity verification, issuance, and use of the common identity standard. It contains two major sections. Part One describes the minimum requirements for a federal personal identity verification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance. Part Two provides detailed specifications that will support technical interoperability of PIV systems of federal departments and agencies. It describes

the card elements, system interfaces, and security controls required to securely store, process, and retrieve personal identity information from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. FIPS-201 objectives are based on HSPD 12 prerequisites, which states that the physical identification card produced in accordance with the Identity Standard must meet four security and reliability requirements: (1) credentials are issued based on sound criteria for verifying an individual employee's identity, (2) credentials are strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation, (3) they can be rapidly authenticated electronically, and, (4) credentials are issued only by providers whose reliability has been established by an official accreditation process.

b. DoD Directives, Regulations and Instructions

PIP Program: DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program," July 19,2004, establishes policy for the implementation and operation of the PIP program including use of identity information, issuance and use of DoD identity credentials, and operation of the Defense Enrollment and Eligibility Reporting System (DEERS), Real-time Automated Personnel Identification System (RAPIDS) and associated systems, DBIDS, Defense Cross-Credentialing Identification System (DCIS), Defense National Visitors Center(DNVC), and the Defense Noncombatant Evacuation Operations Tracking System. The Directive stated that:

> The PIP shall be the Department of Defense's program for: addressing threats to the individual personal privacy of its Members, employees, and beneficiaries; establishing a secure and authoritative process for the 16 issuance and use of identity credentials on the Department of Defense; and ensuring that DoD benefits and access to DoD physical and logical assets are granted on authenticated and secure identity information. (USD [P&R])

IPMSCG and ICAM: Oversight of the PIP Program is delegated to the Identity Protection and Management Senior Coordinating Group (IPMSCG)

under the Assistant Secretary of Defense (Network and Information Integration) (ASD/NII) and DoD Chief Information Officer (CIO) (USD (P&R)). A subcommittee is called Identity Credential Access Management Work Group (ICAM-WG). Its goals are to improve security; enable trust and interoperability; reduce cost and improve efficiencies across the entire federal government agencies (FICAM Roadmap and Implementation Guideline, 2011). The benefits with implementation of ICAM should increase security by closing the gap in area of user identification and authentication, and data encryption. ICAM also should help to bridge the interoperability layer between agencies using different identity credentials such as PIV, CAC. By this, it will enhance the ability to share identity information across agencies.

B. DBIDS

1. Overview

DBIDS is a rules-based access and identity management system that was developed as a force protection program to manage personnel, property, and installation access at DoD installations. DBIDS is deployed as Physical Access Control System (PACS). It is designed as a networked client/server database system to verify the access authorization of personnel entering military installation.

2. Limitation of Current DBIDS Architecture

Currently, DBIDS is a closed system, meaning all collected data are stored in a central database location. The registration process will collect and register individuals who need access to the DBIDS-installed Theater. If military or non-military personnel (such as visitors or contractors) relocate to a different DBIDS-installed base, he or she must register again into DBIDS in order to be granted access. Duplicate identity data are stored in multiple locations and makes it very difficult to manage these data. The current deployed version of DBIDS application does not provide the ability to verify federated credential against its original issuer such as DoD CAC or PIV. With current design, it is

impossible for any interested non-DBIDS vendors to access the DBIDS data. This interoperability shortfall makes DBIDS failed to achieve DoD IdM goals for data sharing across agencies.

Also, current DBIDS credential is not FIPS-201 compliant. DBIDS credentials are issued in multiple formats without any standardized instructions. DBIDS also failed to meet HSPD-12 for the NACI background check requirement. With current architecture, it is very difficult and nearly impossible to implement this functionality to provide the ability to connect to other authoritative data sources for periodic reinvestigation, making DBIDS incompliant with FIPS-201. And, lastly, DBIDS application and DBIDS workstations are not configured to operate with HSPD-12 security feature such as PKI certificates ("DoD Implementation of Homeland Security Presidential Directive -12," 2008).

3. Potential DBIDS with Cloud Computing

Cloud Computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction ("Summary of NIST Cloud Computing Standards Development Efforts," 2010).Cloud computing is often viewed as massively scalable data centers that form an infrastructure capable of remotely running applications and storing data that can be accessed from any connected device over the Internet. Clouds offer a virtual environment for hosting user applications on one or many physical or virtual servers making clouds particularly compelling for applications that have unpredictable usage demands.

Re-architecture DBIDS with Cloud Computing will be a step in the right direction toward the DoD's vision of Identity Protection and Management. With this re-architecture approach, the DBIDS application will be raised to another level as service-centric PACS solution. This will ensure the interoperability for sharing data between DBIDS-installed Theaters. When a DBIDS registered

military personnel has been transferred from one DBIDS installation to another DBIDS installation, that person will not have to register again and all of his or her information will be shared and updated. When a DBIDS registered military personnel needs to access another PACS installed installation, the PACS application in the other installation can use the DBIDS services to get registration information and validate that military personnel credential. In addition, non-DoD personnel will be able to access DBIDS installed installation by asking the DBIDS services to verify his or her identification. This will ensure sharing information across internal government agencies. Non-government institutions can also use the BIDS service to authenticate DBIDS registered military personnel for granting access to their facilities.

A centralized DBIDS credential management process will ensure that the DBIDS credentials will meet FIPS-201 standard requirements with the official accreditation process. With Cloud Computing, DBIDS will become a net-centric service application. This will open the door to other DMDC and federated services such as electronically authenticating PIV, and CAC (compliance PIV) credentials, access to DMDC background screening services, and access to credential prevocational information for security alerts or access to Biometric Task Force (BTF) for ten-print background submissions.

We will discuss in depth the current design of DBIDS and its limitations to fulfill DoD IdM vision, and how to re-engineer DBIDS with Cloud Computing and what this technology can help move DBIDS in the right direction to achieve the DoD IdM current and future goals in the next two chapters.

III. CURRENT DBIDS DESIGN AND IMPLEMENTATION

DBIDS is the largest physical access system in the DoD, providing theater-wide physical access for nearly two million base workers and visitors in Europe and Asia. Soon to be deployed at military bases worldwide, it uses existing DoD-issued identification credentials, including digital photos and digital fingerprints, and over the years, this data collection has become some of the largest stores of biometrics data in the Department. Currently, DBIDS uses this biometric data for one-to-one exact match at Access Point for allowing access privileges. Moreover, these data can be utilized for background screening purpose. DBIDS is scalable to cover a building, checkpoint, installation, or an entire theater of operations. The rule-driven system is configurable by local authorities to meet their access policies, allowing the level of authentication to be determined by threat level or the dictates of the base commander.

A. DBIDS SOFTWARE REQUIREMENTS

1. Business Context

DBIDS is an access control and identity management application and database system used for tracking contractors, vendors, third-party nationals, and any other individuals requiring recurring access to a DoD installation. The Department of Defense Manpower Data Center (DMDC) originally designed DBIDS for force protection.Current versions of DBIDS are deployed at various DoD facilities around the world and are used for assigning privileges according to an individual's access requirements. DBIDS application also provides the ability to manage individual property such as vehicles, bikes, pets and weapons. It will handle five primary functions:

a. Personnel Vetting

DBIDS will ensure affiliation or trustworthiness across the enterprise in near real time, by vetting an individual's identity under Federal

Information Processing Standards Publication (FIPS) 201 (Personal Identity Verification, PIV, of Federal Employees and Contractors, Federal Information Processing Standards Publication 201-1, National Institute of Standards and Technology Gaithersburg, Md., March 2006), using a credential approved by The Under Secretary of Defense for Personnel and Readiness (USD P&R).

b. Access Control

DBIDS will enable the deployment of a secure and strongly resistant, rule-based and rule-driven access control system that is certified and accredited according to the DoD Information Assurance Certification and Accreditation Process (DIACAP) (Department of Defense Instruction 8510.01, November 28, 2007). The DBIDS solution with support of third party options will enable a solution that is mobile and scalable enough to cover a building, checkpoint, installation, or theater of operation.

c. Identity Management

The DBIDS solution will provide digital authentication of identity and be able to rapidly authenticate visitors electronically while adhering to the conditions of Homeland Security Presidential Directive (HSPD) 12. (Policies for a Common Identification Standard for Federal Employees and Contractors, Homeland Security Presidential Directive 12, August 2004)

d. Verification

DBIDS will link to law enforcement databases and other federal and state databases for the purpose of personnel vetting and identity confirmation.

e. Authorization

Authorization describes the process of privileges-assignment to registered DBIDS entities including Person, Organization, and Vehicle. Access privileges will often need to be determined at each facility. However, with a shared DBIDS registry database the registrant will have already been

authenticated and recorded, making it possible to provide the access privileges at the next facility, even at the visitor center or the gate. The DBIDS card produced from identification and categorization can now be used throughout a geographical area sharing a DBIDS registry database as an authentication in order to facilitate registry for local access. Currently, DBIDS registry is available for a single installation only. This is one of the pitfalls of the current DBIDS design since historical, DBIDS was designed to resolve physical access solution for one particular installation. With this design, other installed DBIDS will not be able to share each other information and this is why DBIDS is not compatible with HSPD-12 to ensure interoperability functionalities. The definition about global DBIDS authoritative data source has not been available for the current DBIDS versions.

Figure 1 and associated text describe at a high level the business processes associated with DIBDS, including identity management, access control, and authorization. This diagram is taken from version 2.x of DBIDS User Guidelines.

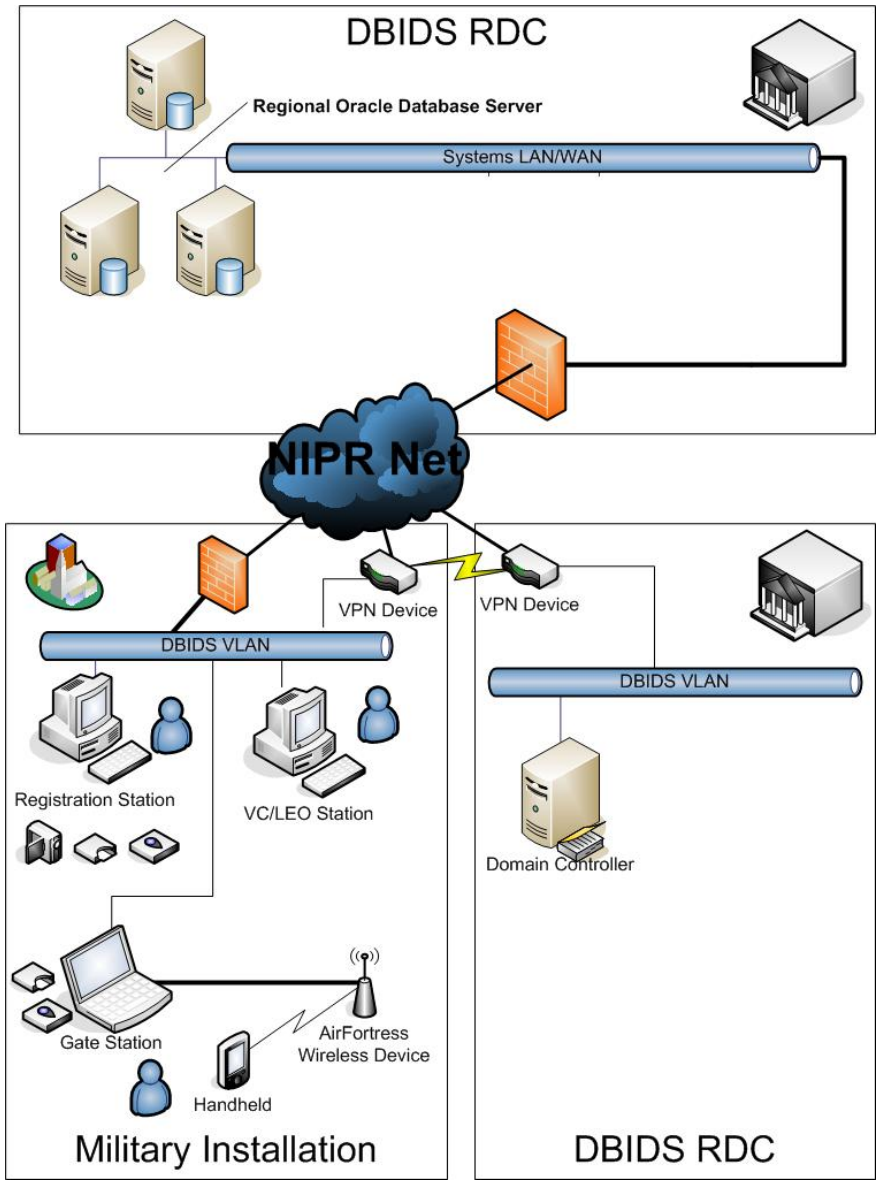

Figure 1. DBIDS Installation Overview
(From DMDC-DBIDS User Guidelines)

A user's interaction with DBIDS begins with establishing a need for physical access to a DBIDS enabled area. This need may be recurring access for a set period, or it may simply be a one-time only access. The first step is to capture relevant registration information through one of the following methods: manual input of registration data, electronic retrieval of data already existing in DBIDS, or parsing data from printed on DoD Credential barcodes.

Once registration data has been captured for an individual, there may be a need to screen an individual based upon local policy. If it is determined that an individual needs to be screened, the appropriate data is submitted by DBIDS to the selected screening partners. Currently, this screening process has not been embedded into DBIDS business process. It happens as a separate one-time background check on an individual who needs access privileges to the installation. Once the security results have been retrieved from these screening partners, an authorized operator can review the results and make a decision of whether or not to grant the individual access. DMDC has been working in the direction of becoming the central repository for rapid electronic authentication. Therefore, DBIDS should utilize these DMDC services to encapsulate, and automate the screening process into DBIDS business process.

DBIDS also supports the use of credentials for identity retrieval and access purposes. A credential is an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. This support for credentials includes the ability to use an existing DoD credential or create a DBIDS-specific credential. Both CAC and DBIDS credentials have barcode39 printed in the back of each card. When using CAC to request for DBIDS-installed access, DBIDS application will store this barcode39 string into its registry to associate the person with his or her identity. At ACP workstation, when an individual present his identity to access, the ACP operator will scan the barcode on his or her credential and DBIDS application will use it to identify his or her record in the registry and using biometric capability to verify if the presented identity credential is matched with the individual.

Once the aforementioned steps have been addressed, the user may be assigned access privileges. When requesting access at a particular control point (either via the workstation or mobile device) these access privileges are used in conjunction with installation-defined business logic to generate an access response, which may be used by a DBIDS operator as appropriate. DBIDS operator can use the “Access and Privileges Management” GUI to select,

and granting an individual access areas, date and time to access on which level of Force Protection. These installation-defined business rules are currently, hard-coded in DBIDS application logics. This is why there are multiple versions of DBIDS currently to support different business rules for different installations. This is another pitfall for the current design. However, some of the upgraded DBIDS versions have been implemented role-based access business rules. This means that DBIDS selects an individual role and base on the selected role, a default access profile will be assigned. The default profile will include default access areas, date and time to access and level of force protection.

2. Functional Requirements

a. Use Cases

These use cases are developed by DMDC-DBIDS Business Analysis (BA) and Development teams who working with DBIDS customers to capture the business requirements for each military installation. Each different military installation might have different business requirements; however, these use cases are the most common cases for a typical access control system. The following use cases are referenced from DBIDS functional document.

- Person Registration Use Case

UC1	Person Registration
Description	This use case details the steps that are taken to manage an individual's account data through the Person Registration module.
Assumptions	• Operator has been authenticated and has the appropriate privileges to manage accounts (i.e., "Privilege to register a person") • Workstation has appropriate hardware installed. • System has a connection to external data sources (e.g., DEERS, external DBIDS regions)

Basic Course of Action	1. Operator opens Person Registration module
	2. System displays empty account
	3. Operator scans credential barcode
	4. System attempts data retrieval while displaying status indicator
	5. System displays retrieved data
	6. Operator manages the following data - assuming they have the appropriate operator privileges.
	  • Identity Data
	  • Biometric Data
	  • Screening
	  • Access Privileges
	  • Credentials
	  • Association Data
	  • Access Roster
	  • Additional Data
	7. Operator chooses to save the entered data
	8. System validates and saves the data

Notes	The initial registration will require that the operator entering the required data in a sequential order. Subsequent edits to this data will allow the operator to jump to data elements as necessary.

Table 1. Person Registration Use Case (From DMDC-DBIDS Functional Specification)

- Access Authorization Use Case

Authorizing access to a facility is another important capability that is managed through the DBIDS application. After Registrants have presented the Registrar with a valid form of identification and that identification is authenticated, access is granted to the authenticated individual based on his or her relationship or the role he or she plays in with respect to the facility for which he or she requests access.

After authentication and registration, the Registrar inputs the facility ID of the facility or facilities the Registrant is requesting access to. The DBIDS application verifies that the facility in question is within the facility domain or span of control of the Registrar. The Registrar inputs the Registrant's reason for needing access to the facilities by selecting list of acceptable reasons in a pull down menu. The System records facility access requested and access reason in the DBIDS Registry. The System applies predefined DBIDS access rules, based on role and reason for access, to determine access level. DBIDS then adds access privileges to the Registrant's profile.

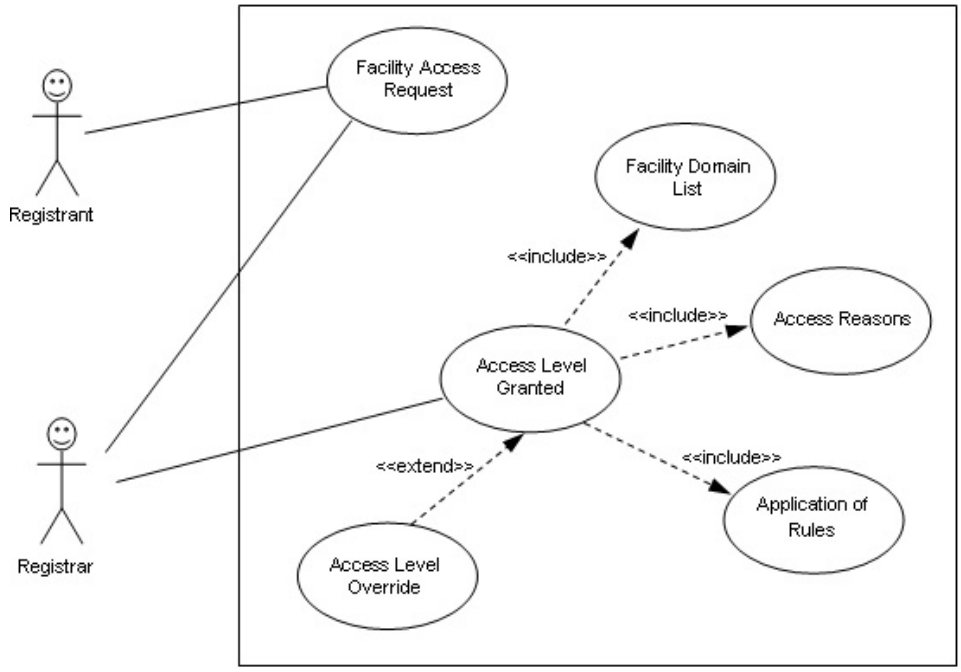

Figure 2. DBIDS Access Authorization Use Case

UC2	Access Authorization
Description	This use case details the steps that are taken to manage access privilege data for an account.
Assumptions	• Operator has been authenticated and has the appropriate privileges to manage access privilege data (i.e., “Privilege to assign access privileges”)
Basic Course of Action	1. Operator selects to manage access privilege data. 2. System displays summary list of existing access privilege sets for current account 3. Operator chooses to add access privileges. 4. Operator enters access privilege data 5. Operator saves changes 6. System logs actions and saves data.
Notes	None

Table 2. Access Authorization Use Case (From DMDC-DBIDS Functional Specification)

- Reports Use Case

The DBIDS application provides the capability to generate and manage reports pertaining to individual and regional sites.

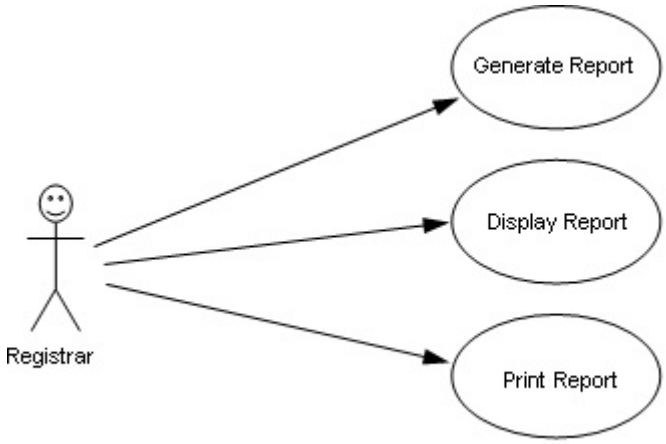

Figure 3. DBIDS Law Enforcement Report Use Case

UC3	Law Enforcement Reports
Descriptions	This use case details the steps that are taken to view reports.
Assumptions	• Operator has been authenticated and has the appropriate privileges to view reports (i.e., “Privilege to manage reports”)
Basic Course of Actions	1. Operator selects to view reports. 2. Operator selects report to view 3. System prompts for input parameters and displays report data 4. Operator closes report
Notes	In future releases we will want to add the ability for operators to perform ad-hoc reporting.

Table 3. Law Enforcement Report Use Case (From DMDC-DBIDS Functional Specification)

b. Additional Features

DBIDS software also allows registering Organization, Vehicle, Pet, and Weapon. In addition, DBIDS software allows the Registrar to capture a variety of biometric data, such as fingerprints, iris (eyes captured), hand-geometry, and voice recognition.

c. Monitoring and Logging Requirements

The system shall log all system-level errors, which should contain the following information: Time/Date, Error, Module, and Stack Trace (if applicable). The system shall have the ability to limit access to log to approve administrative personnel. The system shall log all login attempts, including at timestamp, workstation or MAC address of mobile devices, logged-on operator's information, and success/failure.

The system shall log all logoff actions (date/time, workstation, and operator), the viewing of reports (timestamp, workstation id, operator, report, and parameters), all searches (timestamp, workstation, operator, type, parameters, and result count), all inserts, updates, deletes, and views of access privilege data (timestamp, workstation, operator, user, data modifications).The system shall log all inserts, updates, deletes.

Currently, DBIDS will store this logging information locally at DBIDS registry for administrative reporting services. This logging information is also used for trouble-shooting DBIDS field issues.

3. Non-Functional Requirements

a. Performance Requirements

The system shall ensure the retrieval of data using a credential scan at the control point takes no longer than two seconds on average. The system shall ensure that each region shall be able to support 100,000+ records.

b. Security Requirements

The system shall comply with FIPS, PUB 140–1 (Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication 140–1, National Institute of Standards and Technology Gaithersburg, Md., 11 January 1994). The system shall comply with FIPSPUB112 (Password Usage, Federal Information Processing Standards Publication 112, National Institute of Standards and Technology Gaithersburg, Md., 30 May 1985). The system shall support the ability to encrypt data “at-rest.” The system shall support the ability to encrypt data “in-transit.”

c. Graphic User Interface (GUI) Requirements

The system shall have appropriately ordered tab sequence for all input forms. The system shall support the use of “Hot-Key” shortcuts for appropriate menu items and buttons. The system shall display confirmation messages for all data input screens if the operator attempts to close the screen without saving.

B. CURRENT DBIDS SOFTWARE DESIGN AND ARCHITECTURE

1. Architecture Logical View

Figure 4 presents a logical view of the DBIDS application and shows the application’s connection to external sources for vetting. DBIDS application is designed and developed using Microsoft Visual Basic 6.0 Technology. It contains a set of Windows forms. All business logics and presentation logics are bundled together in the same form codes. Data will be stored on the regional DBIDS Oracle Database server. At each DBIDS installation, one registry database server is used to store all DBIDS registration.

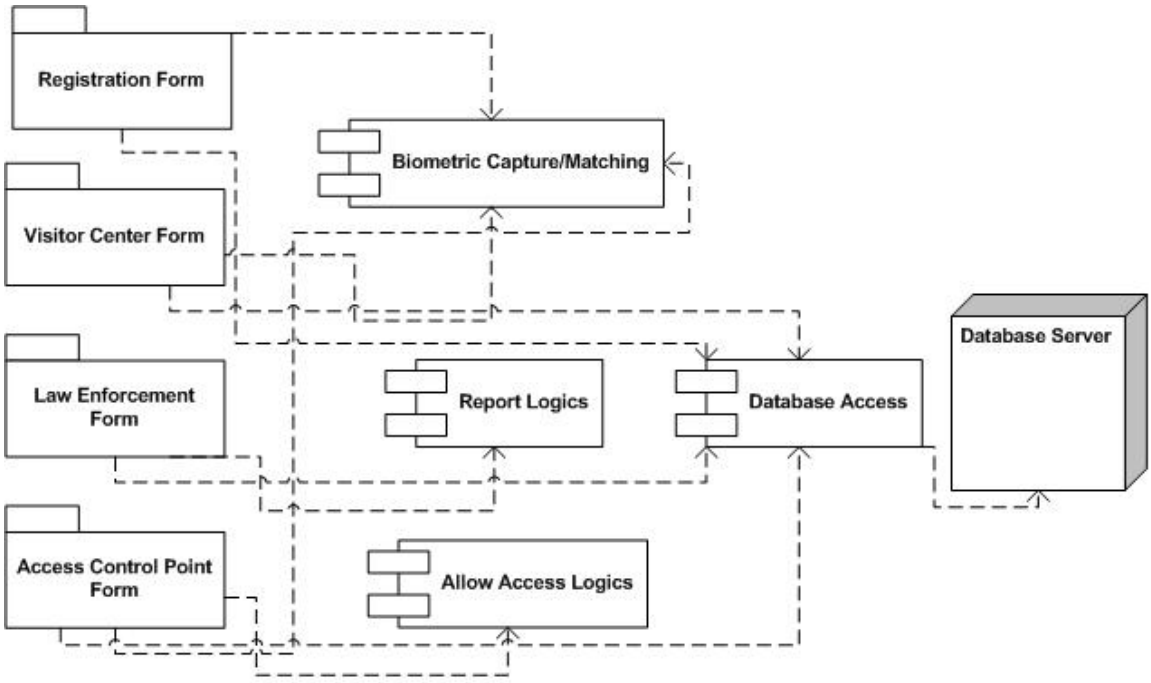

Figure 4. DBIDS Components Logical View

2. DBIDS Workstations

The DBIDS system utilizes four types of workstations, each designed to perform specific tasks:

- Registration Center: The Registration Center workstation enables an operator to enter a person's information into the database either by scanning an identification card to retrieve the barcode-stored data, or by manually typing information into data field boxes.
- Control Point: Control Point machines are located at installation Access Control Points to authenticate persons entering the installation.
- Visitor Center: The Visitor Center allows for validating authorized personnel, and for sponsors to register escorted and authorized guests onto the installation.
- Law Enforcement: Law Enforcement workstation allows for complete monitoring of personnel actions and authorities by any law enforcement activity. It is also used to allow the DBIDS administrators to set individuals' status as

“Barred,” “Suspended,” or “Wanted.” In addition, DBIDS administrators can generate document style reports.

DBIDS software application can be configured to be different types of workstations. Each workstation type consists of different set of business processes. Different software logics are designed and implemented to execute these required business process. These logics are encapsulated within DBIDS software. This is also a problem when deploying DBIDS software. Deployed Registration workstation module will also contain executable codes for other type of workstations.

C. PROBLEMS WITH CURRENT DBIDS DESIGN

The current DBIDS design combines the business layers and the presentation layer into .NET components and the software is deployed into desktop workstations, which create the following problems:

- Multiple software versions of DBIDS to support different DBIDS customers’ business requirements creating version control nightmare.
- Does not provide an easy way to interface with existing DMDC services such as Automated Data Repository/Automated Data Warehouse (ADR/ADW).
- Does not provide a capability to interface with other governmental and federated cross credential services, such as Biometric Fusion Center-Automated Biometric Identification System (BFC-ABIS), Federal Bureau of Investigation-Integrated Automated Fingerprint Identification System (FBI-IAFIS), and Federation for Identity and Cross Credentialing Systems/Defense Cross-Credentialing Identification System (FiXs/DCCIS).
- Does not support multiple platforms, and multiple software versions for existing DBIDS customers with different requirements.

- Does not create a common platform, which will become the primary CONUS and OCONUS BIDS infrastructure over time.
- User registration and resource access authorization functionalities are coupled into a single software package, making it difficult for potential vendors to utilize DBIDS captured data: such as accessing individual's registration or authorization data for different purposes.
- Does not provide the ability to remotely distribute software patches and upgrades.
- Does not have centralization of global DBIDS databases so that different installed DBIDS can share data among regions.
- Does not have modularization of codes.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. DBIDS DESIGN WITH CLOUD COMPUTING

The current DBIDS application does not separate the core business layer from the presentation layer: this tight coupling has made DBIDS software hard to extend and complicated to maintain. In this chapter, we attempt to address the problem of tight coupling by introducing a new DBIDS design using Cloud Layer Architecture. Figure 5 shows the summary components of architecture layer.

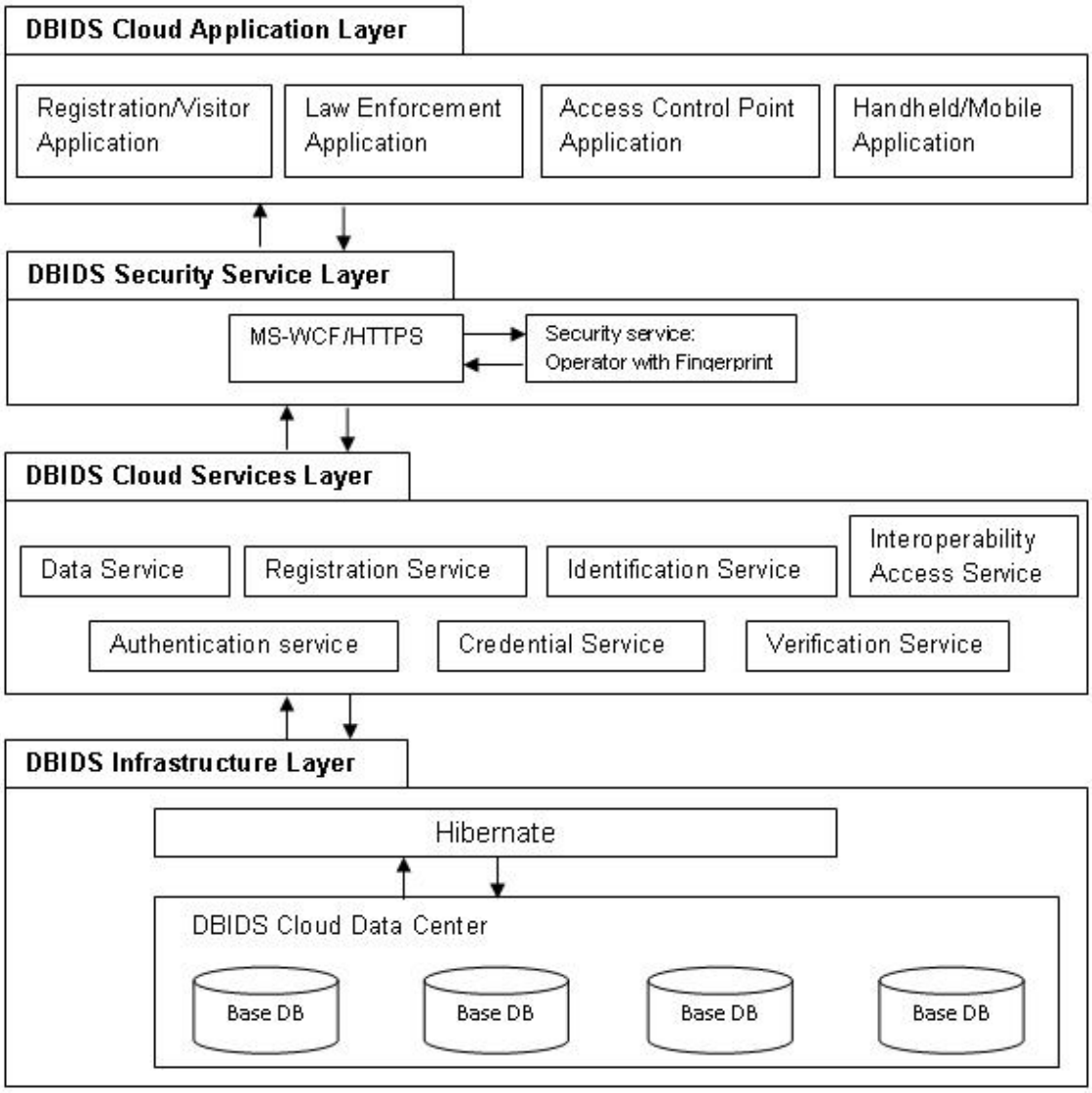

Figure 5. DBIDS Private Cloud Architecture View

A. DBIDS CLOUD SERVICES LAYER (SAAS)

Promoting the evolution of DBIDS into a global enterprise solution, we propose that DBIDS be designed with loosely coupled interfaces between application tiers. By decomposing core functions as service components, it is possible to reuse implementations across releases of DBIDS. These are designed as standard Web services, which are available for internal and public usage. Internally, DBIDS functionalities such as person registration, person access authorization, or credential verification can be implemented as services and DBIDS client applications can consume these services as needed. As example, registration workstation application can use registration services to register persons. Meanwhile, control point workstation application can use access authorization and credential verification services to check for individual's access permissions. The currently DBIDS application has added the functionality to verify a DoD Credential through the Defense Enrollment Eligibility Reporting System (DEERS) by using an add-on proxy during the registration process. This functionality can be decomposed and made as part of the DBIDS cloud services. It can be used by the DBIDS law enforcement application to perform continuous background check on individual who has been granted access to the installation. The service also can be used externally by other vendors' application to verify DoD credentials. For example, DBIDS hardware vendors can utilize DBIDS cloud services to access registrants' data for building pedestrian access turn-style solution.

1. DBIDS Cloud Services

This is the business layer consisting of the authoritative data store and core business logic necessary to maintain base and facility level registries of a population and Registrants' security privileges within the base/facility. The services provided by this layer include identification, authentication, verification, credential, and registration and data service. Table 4 lists general description of each proposed core services. These services can be utilized and consumed to

build various applications to fulfill DBIDS requirements. These applications can be Registration Management, Law Enforcement, Access Control Point Management, and more.

Component	Description
Registration Service	Provide functions to add/update individuals PII information into registry by credential identifier, or personal identifiers
Data Service	Communicate to Data Access Layer, a database factory class implementation paired with business object adapters to form the business object layers
Authentication Service	Provide functions to authorize individuals, their sponsors, and vehicles if they have access privileges to the installation using their different identities.
Identification Service	Provide functions to identify if a DBIDS registered individual base on their identities.
Verification Service	Provide functions to verify if an individual present the corrected assigned identity.
Credential Service	Provide functions to produce PIV compatible DBIDS credential.
Interoperability Access Service	Provides functions to access DEERS or other Federated data sources using CAC token or FASC-N.

Table 4. Web Services Component Description

B. DBIDS SECURITY SERVICE LAYER

DBIDS Web Services and Windows Communication Foundation (WCF) services use the Hypertext Transfer Protocol Secure (HTTPS) and Microsoft Message Queuing (MSMQ) protocol to communicate.

The HTTPS protocol is used to ensure all communication between client and server is encrypted when a service call is made. DoD certificates must be issued to all applications hosting and exposing a service implementation. The MSMQ protocol is used for communication between systems and sub-systems when the interface requires reliable and durable message delivery in environments for which the network is intermittently connected. MSMQ is an application layer protocol that works on top of Microsoft Remote Procedure Call (RPC).

As another layer of security, operator login information, which includes operator ID and operator Fingerprint data (shown as security service in Figure 5), will be embedded into each endpoint of the request. A DBIDS Web service request, sent from either the DBIDS application or another third-party software package, must have a valid (i.e., registered) operator in the DBIDS database. The request will then be parsed by the DBIDS application to validate if the sending operator has the privileges to access DBIDS Web Services.

C. DBIDS INFRASTRUCTURE LAYER (IAAS)

This is the DBIDS global database layer, which collects all identities registered to individual DBIDS installations. Its flexible system configuration allows the same components in the base repository tier to be deployed as a regional level repository or a base-level repository, that is, one instance of a Base Repository system may provide services for either an individual base or facility deployment, or multiple bases and facilities within a geographic region. Bases and facilities that share a Base Repository system also share the population registered in the Base Repository. As shown in Figure 5, these

repositories are placed in the DBIDS Infrastructure layer to create DBIDS data center to support multiple DBIDS deployed regions.

1. Oracle Cloud File System Solution

According to the National Institute of Standards and Technology, three key characteristics of a Cloud Technology are resource pooling, broad network accessibility, and rapid elasticity. Oracle Cloud File System comprises the following features: Oracle Automatic Storage Management Cluster File System and Oracle Automatic Storage Management Dynamic Volume Manager. It has the following characteristics:

- Providing shared pooled storage with unified namespace for applications, operational files, and user files
- Accessing storage either directly over a storage network or over traditional networks
- Rapidly growing, shrinking, and migrating storage pools while applications are online
- The Oracle Cloud File System provides advanced data management and security features including:
    - Snapshots and replication of files and file systems for backups and disaster protection;
    - Data access security and encryption to protect from security threats;
    - Easy aggregate management operations via file tags;

2. Hibernate

We recommend using Hibernate technology for object mappings of the DBIDS data models, because it provides all the features to quickly build an advanced persistence layer in code. Hibernate supports caching and transactional capabilities, which will enhance the quality of DBIDS data. The Hibernate helps reduce the burden for developers by providing much of functionality and let developers concentrate on business logic. In addition,

Hibernate provides a much easier way to develop a cross platform application regardless of different types of database software products.

Hibernate is a part of the ORM (Object Relational Mapping) technology originally developed on the Java platform. The Hibernate framework supports rapid development of a data access layer without requiring a substantial portion of “cookie-cutter” code to be implemented. In lieu of writing stored procedures and individual code functions to translate the results into domain objects, Hibernate defines a mapping file language using XML to be used to define the relationships between database tables and domain objects. The Hibernate framework assemblies execute the mapping of the files, construct the queries and translate results for each domain object without specific code functions being developed.

3. Database Design

Oracle 10G is the database technology used across all application tiers. The base repository tier systems utilize Oracle 10G Enterprise, while the Cache tier systems utilize Oracle 10G Standard. The service implementations of the Global Web Services sub-system requires access information stored in the Global Registry DB database instance. Using the Oracle JDBC driver, the service implementations execute SQL-based calls to store and retrieve data (Figure 6).

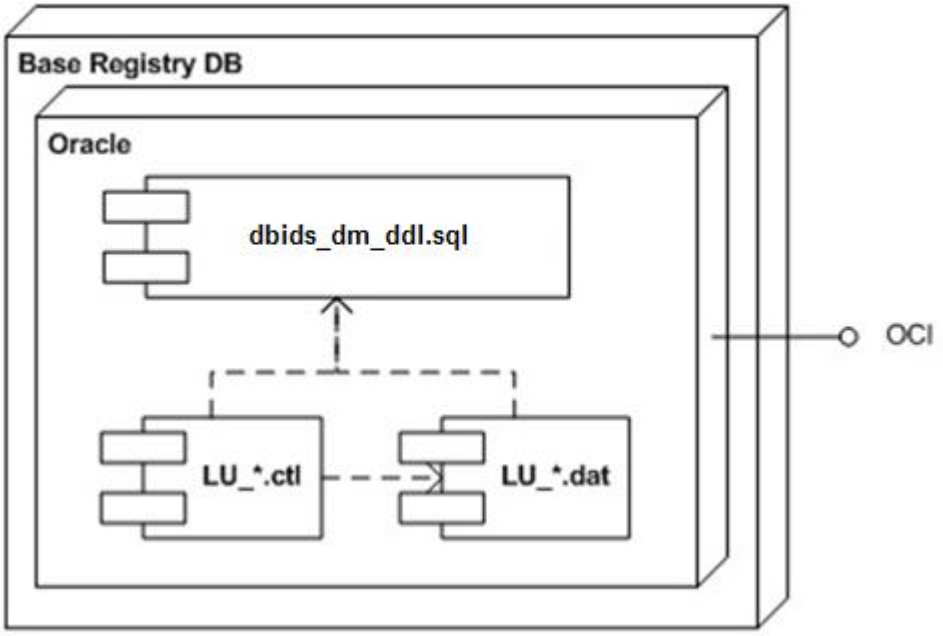

Figure 6. DBIDS Database Component Diagram (After DMDC-DBIDS Technical Specification)

The Base Repository DB contains the following components:

- Oracle product: installation and configuration of the Oracle Standard database server
- Package “dbids_dm_ddl.sql”: tables, indices, relationships and store procedures necessary to support the persistence of registration, authentication, verification, identification, credential information.
- Control files LU_*.ctl: SQL loader control files that load the control and lookup data store in the data files.
- Data file LU_*.data: control and lookup data files that contain the set of control and lookup data.

(a) Database Design Decision

Each of table in the DBIDS DB must have a primary key. A primary key for person information table (PN table) is called BIDS_ID. This is a unique identifier among all DBIDS installations.

Oracle 10G or above will support BLOB field to store fingerprint and photo images. Also, credential data such as FASC-N (Federal Agencies Smart Credential Number) and CHUID (Card Holder Unique Identifier) are stored as BLOB fields.

Each table must have row creation date (ROW_CRT_CDTTM) and row update date (LAST_MOD_CDTTM), and installation identifier string (INST_ID) and last modified operator name (LAST_MOD_BY). This helps provide for audit functionalities.

(b) Database Design Detail

The tables in DBIDS database can be categorized in these areas:

- Personal information: This includes tables to store person demographics data, person address, and phone and person status.
- Personal issued credentials: This includes all credential data for a person include issued and expiration date, and barcode, and status information.
- Personal biometric: This includes tables to store person fingerprint data, person photo data, and person iris data.
- Personal Authorization information: This includes tables to store person authorization profile data with days, time, and areas or facilities and force protection condition which allowed person to access.
- Personal property information: This includes tables to store person vehicle, pet, weapon, and bike data.

- Operator management information: This includes tables to store data for different types of operator, his or her username and password.
- Lookup information: This includes tables to store mapping codes and descriptions.

D. DBIDS CLOUD VIRTUALIZED APPLICATIONS

This is the presentation layer of DBIDS Cloud. These Windows .NET applications will be the GUI software designed to consume DBIDS Cloud Services. Figure 7 show DBIDS applications component diagram for building DBIDS applications such as Registration, Access Control Point, Law Enforcement, and Handheld. These applications will use the Composite User Interface Application Block (CAB) framework - a common shell application that is implemented for all thick-client workstation applications. Functional requirements are introduced into the shell through modules, where each module may be loaded dynamically at runtime, based on configuration and user permissions. Reuse of common components is achieved through the inclusion of an Infrastructure module. In futures, these applications should be implemented as thin-client applications, which can be access through a web-browser.

For mobile devices, it makes sense to implement a lightweight thin client application to consume DBIDS access authorization services. The thin client application will display a colored result to operators to indicate if the person is granted for access.

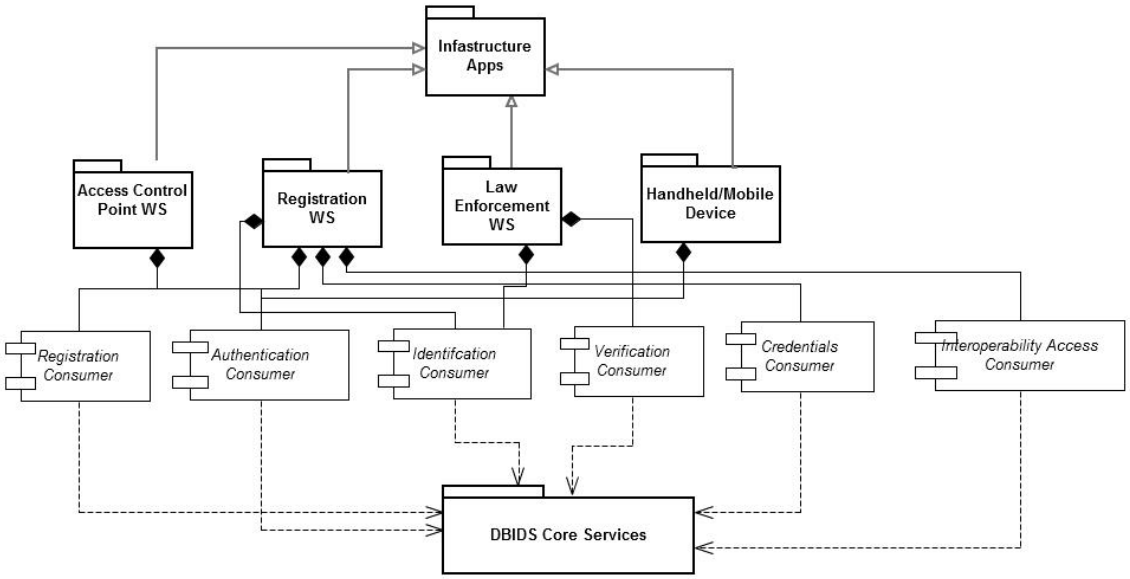

Figure 7. DBIDS Virtual Applications Component Diagram

The use of Layouts, Workspaces and SmartParts provides a modular GUI architecture for the DBIDS application. A hierarchy of layouts is used by the DBIDS application. A single core layout is loaded by the Infrastructure. The Layout module provides the base set of menus, toolbars, and workspaces for use by the rest of the application. Modules that require more complex screen arrangements provide additional layouts.

Layouts are loaded into a workspace as a hierarchy containing layouts. Figure 8 illustrates the hierarchy of the layouts.

Figure 8. DBIDS Virtual Applications GUI Layout Component (From DMDC-DBIDS Technical Specification)

These applications will be installed and deployed onto all Virtual workstations and mobile devices so that DBIDS users will not have to worry about the deployment and upgrade challenges. Some of the examples of these available applications are Registration, Sponsorship & Background Screening, Identification Credential Issuer, Electronic Biometric Enforcement Process, Access Management, and “Be on the Lookout (BOLO) Message.” Depending on the privileges of the sign-on operator, some of these applications will be available for usage. All workstation applications require authentication and authorization of users by enabling CAC-logon.

E. DBIDS CLOUD VIRTUALIZED WORKSTATIONS

Currently, DBIDS deploys two types of workstation: Registration workstations and Access Gate workstations. A Registration workstation provides operators the ability to manage registry and base configuration data. An Access Gate workstation provides the access transaction capabilities. Gate-type workstation systems support an offline/disconnected mode, while Registration systems do not. Virtualization workstation is one alternative solution that can help provide for these workstations’ functions and reduce the cost for maintenance and upgrade, while providing greater control over PC resources and stronger IT security. The deployed DBIDS workstation images will be created and managed centrally, making the DBIDS software upgrade task far less complicated. Updated DBIDS workstation images can be uploaded centrally, saving many person-hours by eliminating the need for DMDC DBIDS support team to physically install upgrades for all deployed workstations. In addition, all DBIDS data will be stored centrally at security location, and group security can be easily applied for all operators’ access rights.

1. Desktop Virtualization Technology

Workstation virtualization uses hypervisor technology, a type of software that allows multiple operating systems to run concurrently on a host computer, to decouple an operating system from its host hardware, and isolate the specific

client environment from other operating systems running on a physical device. This model is generally recognized as virtual desktop integration (VDI).

Centralized Virtual Desktop, a form of server-based computing that uses a “server grade” hypervisor to host multiple unique and isolated client operating systems aboard a single server or group of servers in the datacenter. Virtual desktops are delivered to end-users’ devices via the NIPRNET.

Distributed Virtual Desktop, which runs on a “client grade” hypervisor, is a virtual machine that resides on the local client hardware, such as a laptop computer.

2. Virtualized Development/Testing Workstations

Current DBIDS development environment requires at least a Windows 7 operating system with common development tools such as Visual Studio, database tool (Toad for Developer), XML parser, and others. In order for a DBIDS developer to debug and develop the application, he or she needs a connection to a web server, which exposes all DBIDS Web Services for all DBIDS business functions. In addition, a developer needs a connection to a centralized Database server in order to save test data. Just like the development environment, the DBIDS testing environment also needs at least three Windows operating workstations in order to simulate the real deployed scenario in production.

Virtualization is a perfect solution for this. VMware Workstation enables developers to store any number of standards x86-based configurations as virtual machines, already loaded with any of a wide range of Windows and Linux operating systems, browsers, and other applications. Developers and testers can use these virtual machines, instead of physical hardware, to develop and test multitier applications on a single piece of hardware. Because virtual machines are software entities, they can be readily copied, cloned, reset, and reused with a sequence of mouse clicks. DBIDS Development and QAs teams can create a repository of pre-loaded virtual machines in every desired configuration. Each

machine requires just a single setup. Individual developers can load, on a single machine, a clean “just-installed” configuration they need, by downloading the appropriate virtual machines and networking them virtually.

3. Centralized Virtual Deployed Workstations

Currently, DBIDS software is deployed in various DBIDS workstations such as DBIDS Registration workstation, DBIDS Law Enforcement workstation, DBIDS Gate Access workstation, and DBIDS Visitor workstation. Often, within a customer DBIDS base or installation, there are multiple registration workstations, multiple gate access workstations, and multiple visitor workstations.

VMWare Views virtualization software could serve as a means for bringing all deployed DBIDS workstations into a private DBIDS cloud. With VMware View 4.5, DBIDS desktop administrators can virtualize the operating system, DBIDS applications, and deliver the latest in desktops to DBIDS customers. From a central location, DBIDS administrators can deliver, manage, and update all of DBIDS workstations and DBIDS applications on the order of minutes.

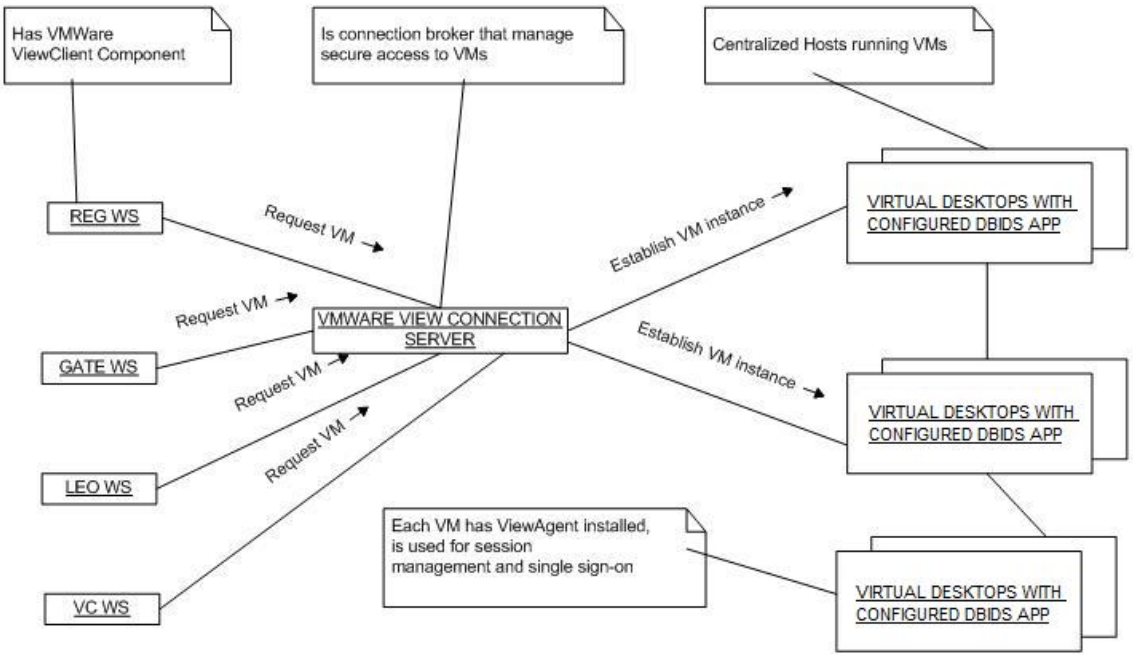

Figure 9. DBIDS Virtualized Workstations Diagram

VMware View includes the following key components: View Connection Server, View Agent, View Client, and View Composer. Figure 9 shows the View Connection Server component, which is the connection broker that manages secure access to virtual desktops and works with Virtual Center to provide advanced management capabilities. It is installed on a Microsoft Windows Server 2003 server that is part of an Active Directory domain. View Agent component runs on each virtual desktop and is used for session management and single sign-on. With View Client, this component supports optional USB device redirection. This agent can be installed on a virtual machine template so that virtual desktops created from that template automatically include the View Agent. When users connect to their virtual desktops, they are automatically logged in using the same credentials they use to log into their domain. If the virtual desktop is not part of a domain or is part of a domain with which no trust agreement exists, single sign-on is not available and the user must manually log in to the virtual desktop. The single sign-on capability can be disabled in View Agent which means that users are always required to manually log onto the virtual desktop. View Client component runs on a Windows PC as a native Windows application and allows users to connect to their virtual desktops through View. This component connects to a View Connection Server and allows the user to log on using any of the means supported for performing the authentication task. After logging in, users can select from the list of virtual desktops for which they are authorized. This step provides remote access to their virtual desktop and provides users with a familiar desktop experience. View Client also works closely with View Agent to provide enhanced USB support. Basic USB support (such as USB drives and USB printers) is supported without View USB support, but View extends this support to include additional USB devices. You can specify View USB support in View Client during the installation. View Composer is used by View to create and deploy linked clone desktops from Virtual Center. The linked clone feature enables View administrators to rapidly clone and deploy multiple desktops from a single centralized base image, called a Parent VM. Once the

desktops have been created, they remain indirectly linked to a snapshot residing on the Parent VM. The link is indirect because the first time one or more desktop clones are created, a uniquely identified copy of the Parent VM is also created. All the desktop clones are anchored directly to the replicate and not to the Parent VM.

4. DBIDS Workstation Virtualization Benefits

Vitalizing the DBIDS Workstations will result in the following benefits:

- Reduce costs and complexity: with virtualization, cost for hardware can be reduced by having multiple physical servers and desktop on fewer machines.
- Reduce cost for DBIDS deploy and upgrade: Current, DMDC is responsible for managing deployed workstation desktops at the physical site. This effort placed enormous pressure on DMDC support staffs. Virtualization can help to reduce maintenance efforts and support costs since DBIDS installed workstations can be retrieved via virtualization workstations.
- Consume less power: able to use less energy on DBIDS workstations.
- Improve security and compliance: Virtualization minimizes risk and data loss. Storing data on central servers and managing them in the data center significantly reduces the security and compliance risks associated with having huge amounts of data residing on local workstations.
- Effective backup and recovery: Virtualization extends virtual infrastructure capabilities to the desktop and server for improved backup, failover and disaster recovery capabilities.
- Increase user productivity by performing daily tasks faster and easier: Virtualization helps balance performance and

turnaround response time by diverse workloads and application requirements.

- Easier for DBIDS support staffs to maintain DBIDS software versioning: all deployed DBIDS application will be upgraded remotely.
- Easier for DBIDS support staffs to remotely logon and capture a snapshot whenever a workstation report a problem. This is so helpful since DMDC support team can easily diagnosis the real-time issues by looking at the run-time DBIDS application.
- All DBIDS registration data is stored on network storage, which centrally controlled and regularly backed up.
- DBIDS administrators on centralized servers manage all configuration details. There is no need to push DBIDS software or other needed software upgrades to all workstations anymore.

F. VENDORS VIRTUALIZED APPLICATIONS

VMware ThinApp software virtualization separates DBIDS applications from the underlying operating systems for increased compatibility and streamlined application management. DBIDS applications packaged with VMware ThinApp can be run in the data center where they are accessible through a shortcut on the virtual desktop, reducing the size of the desktop image and minimizing storage needs. Since VMware ThinApp isolates and virtualizes applications, multiple applications, or multiple versions of the same applications can run on the virtual desktops without conflict. Applications are assigned centrally through View Manager, ensuring that all user desktops are up-to-date with the latest application versions.

With additional support of VMWare ThinApp, any vendor can easily create Physical Access Control System (PACS) software, which can utilize DBIDS

Cloud services to connect to DoD external systems to provide better solution for background vetting before giving access rights to an individual. These applications can be packaged and deployed on the DBIDS virtual workstation and can be available for all DBIDS Cloud users.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND FUTURE RESEARCH

A. SUMMARY

In this thesis, we study and analyze the design and workflow of the current DBIDS architecture. That architecture has made product management of DBIDS challenging and DBIDS's incompliance with FIPS-201 Directives. We discuss how DBIDS can be re-architected to leverage cloud computing with three layers of DBIDS services: DBIDS Cloud Services layer, DBIDS Infrastructure layer, and DBIDS Security Service layer. Re-architecture DBIDS with Cloud Computing will enhance DBIDS's compatibility with HSPD-12 and FIPS-201 Directives. This recommended architecture will serve as a blueprint for new generation of DBIDS application. It will help DBIDS move a step closer in the right direction of DoD's vision of Identity Protection and Management, and DBIDS application will be raised to another level as service-centric PACS solution. DBIDS Cloud provides services for other PACS solution to communicate, exchange, share data, work together to achieve DoD IdM goals.

The proposed SOA-based architecture focuses on decoupling the business layers from the presentation layers. The DBIDS Cloud Services layer contains DBIDS' core functionalities. The functionality can be structured as Web Services, which are published to be used by DBIDS' internal applications and third-party applications. The business layer becomes a SaaS layer in our proposed architecture for the DBIDS private cloud. Re-architecture DBIDS based on SOA principles of reusable, formal contract, loosely coupled, abstraction, compostable, autonomous, and discoverable will provide DBIDS continual opportunities for reuse existing functionalities and create flexibility to expand DBIDS with new requirements.SOA also takes DBIDS in the right path for interoperable with other federation services within DMDC and other agencies.

DBIDS Cloud contains DBIDS applications to fulfill user needs of DBIDS registration, access management, and biometric enforcement, screening and

report capabilities. These applications run on virtual machines, which are preinstalled, configured, and ready to use. Users can log onto these virtual machines using the enabled CAC logon. The applications are .NET Windows-compliant using Microsoft CAB technology. These GUI applications consume DBIDS Cloud Services to provide tools for DBIDS operators to perform DBIDS functions.

Another layer in the DBIDS cloud layer is the Infrastructure layer, which is used to store DBIDS registered data in a central location. Another set of Web Services are also created for data access so that in the future, any application that attempts to access these data can provision the appropriate Web Services.

In addition, the DBIDS Cloud also provides a virtualized environment for developers and testers to exercise and test their products before integrating the products into the DBIDS Cloud.

B. FUTURE WORK

1. Cloud Security

Preventing information leakage is a key concern of both users and providers of cloud services. Our architecture needs to be further reviewed and refined to address security requirements, such as those introduced by Bret Michael and George Dinolt (“Establishing Trust in Cloud Computing,” 2010). When PII data are stored in a massive central repository on a “network,” which can be accessed and consumed by “supposed trusted” vendors’ applications, data security is consistently the top concern. According to Bret Michael and George Dinolt, good security policy can help prevent unauthorized access to central PII data storage and also prevent data damaging leaks such as Wikileaks incidents.

So, extended research about how future DBIDS Cloud can determine data access authentication to decide who to trust to do what should be done to address DBIDS Cloud security concerns. Different applications, different services from different vendors with different role can have different privileges to access

and consume different DBIDS SaaS services. DBIDS Cloud customers must present an identity according to DBIDS Cloud security policy in order to be authenticated and allowed to connect to DBIDS Cloud.

Additional research about different mechanisms to authenticate DBIDS Cloud customer identity should be helpful for addressing Cloud security. Different potential mechanisms like single-sign-on infrastructure, PKI infrastructure, Biometric authorized technology should be studied and experimented.

2. Scaling-Up

Cloud computing technology promises to bring benefits to DoD IT users. However, our architecture needs to be vetted to make sure it will support scaling up the cloud-service support to all 3.5 million DoD IT users. For instance, it is not known what impacts our architecture might have on file system requirements, such as those pointed out by Alex J Nelson (“A Security and Usability Perspective of Cloud File Systems,” 2011). Millions of users on DBIDS Cloud over time will result in petabytes of information. Pet-scale systems introduced problems related to decision-making and usability surrounding system purges and associated data loss and data integrity. Other issues will also rise, like file lookup problem, system performance, and trusting the system. Purge threat and fear of data loss are the most pressing concern of all. This threat is often resulted in a mass deletion of least accessed files triggered when the non-backup parallel system filled up.

A new concept has been introduced and researched to handle this large-scale storage system is called object-based storage-devices (OSD). An OSD is a network-attached storage device which presents an interface for arbitrarily-named data objects of variable size rather than sequentially numbered fixed-size blocks, to deal with the data storage details, such as request scheduling and data layout. Metadata is managed separately by one or more specialized metadata servers (MDSs), which is critical to scalability, reliability and security. The separation of data and metadata storage and management provides very high

access bandwidth to the large-scale distributed storage systems (“A Security and Usability Perspective of Cloud File Systems,” 2011).

3. Web-Based Services (Thin Client Layer)

The architecture of DBIDS should accommodate new requirements. A Private DBIDS Cloud may be transformed into a Community Cloud or Public Cloud to enable the sharing of data among government enterprises. BIDS should provide the capabilities for DBIDS users to access their application running on the DBIDS Cloud Infrastructure through a web browser and thin-client interface, while detecting and managing the emergent cross-domain behaviors that arise in the context of web-based services. Our architecture needs to be further studied to determine whether it sufficiently supports the emergent behaviors, we want to have the services exhibit.

Our proposed architecture with Cloud Computing can make it easy to build DBIDS mobile device applications to support DBIDS Access Point functionalities. These are applications can be developed and deployed on the DBIDS Cloud and can “click” to download, “click” to install and “click” to run. Different DBIDS mobile device applications can be used to support different mobile devices from different vendors. This will certainly extend the capabilities of DBIDS and it helps resolve hardware dependence challenges. However, this means that DBIDS will have to support multiple versions of DBIDS mobile device applications on the Cloud. And DBIDS mobile device operators must be trained to have knowledge of each application. What about the idea of DBIDS Mobile Web applications through a user-familiar web browser? DBIDS Mobile Web application is another research area which can help to extend the ability of DBIDS functionalities and DBIDS Cloud capabilities.

LIST OF REFERENCES

Amazon.com. (2011). Amazon simple storage service (Amazon S3). Retrieved on April 05, 2011, from http://aws.amazon.com/s3/

Cloud computing. (n.d.). In Wikipedia. Retrieved on February 02, 2011, from http://en.wikipedia.org/wiki/Cloud_computing

Cloud Security Alliance. (2010). Top threats to cloud computing v.1.0. Retrieved on March 15, 2011, from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cloud Tweaks. (2008). Cloud computing – demystifying SaaS, PaaS and IaaS. Retrieved on February 07, 2011, from http://www.cloudtweaks.com/2010/05/cloud-computing-demystifying-saas-paas-and-iaas/

Chou, D. (2009). SOA and cloud computing. Retrieved on April 08, 2011, from http://www.slideshare.net/davidcchou/soa-and-cloud-computing-2647186

Friedman, A., & West, D. (2010). Privacy and security in cloud computing. Retrieved on April 12, 2011, from http://www.brookings.edu/~/media/Files/rc/papers/2010/1026_cloud_computing_friedman_west/1026_cloud_computing_friedman_west.pdf

Gillett, Frank. (2008). Future view: The new tech ecosystem of cloud, cloud service, cloud computing. Retrieved on February 02, 2011, from http://soft.ssu.ac.kr/Arial/Courses/CurrentSemesters/2011/Service%20Oriented%20Architecture/06.%20Cloud%20Computing.pdf

Hanna, S., Juniper Networks. (2009). Cloud computing: finding the silver lining. Retrieved on May 09, 2011 from http://www.ists.dartmouth.edu/docs/HannaCloudComputingv2.pdf

Johnston, S. (2010). Taxonomy: The 6 layer cloud computing stack. Retrieved on February 02, 2011, from http://samj.net/2008/09/taxonomy-6-layer-cloud-computing-stack.html

Linthicum, D. (2009). Finding the intersections of SOA and cloud computing. Retrieved on February 10, 2011, from http://www.soa-consortium.org/podcasts-webcasts/DC-2009/podcast-dl.htm

Michael, B., & Dinolt, G. (2010). Establishing trust in cloud computing. Retrieved on June 02, 2011, from http://iac.dtic.mil/iatac/download/Vol13_No2.pdf

Nelson, A., Dinolt, G., Michael, B., & Shing, M. (2011). A security and usability perspective of cloud file systems, in *Proceedings of the 6th IEEE International Conference on System of Systems Engineering*, Albuquerque, New Mexico, June.

Nielsen, R. and Hamilton, B. (2004). Observations from the deployment of a large scale PKI. Retrieved on June 20, 2011, from http://middleware.internet2.edu/pki05/proceedings/nielsen-large_pki.pdf

Platform as a service. (n.d.) In Wikipedia. Retrieved on February 04, 2011, from http://en.wikipedia.org/wiki/Platform_as_a_service

Raines, G. (2008). Cloud computing and SOA (Technical report no. MTR090026). The MITRE Corporation. Retrieved on February 10, 2011, from http://www.mitre.org/work/tech_papers/tech_papers_09/09_0743/09_0743.pdf

Rao, N. (2011). Arguments for SOA in cloud computing environment. Retrieved on June 08, 2011, from http://soa.sys-con.com/node/1338494

Software as a service. (n.d.). In Wikipedia. Retrieved on February 06, 2011, from http://en.wikipedia.org/wiki/Software_as_a_service

Wardley, S. (2008). Cloud recap … The cloud today. Retrieved on April 20, 2011, from http://blog.gardeviance.org/2008/10/cloud-recap.html

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Professor James Bret Michael
   Naval Postgraduate School
   Monterey, CA

4. Professor Man-Tak Shing
   Naval Postgraduate School
   Monterey, CA

5. Professor Thomas Otani
   Naval Postgraduate School
   Monterey, CA

6. Mr. John Shea
   Office of the DoD CIO
   Alexandria, VA

7. Mr. Scott J Dowell
   Computer Science Corporation
   San Diego, CA

8. Dr. Jeffrey Voas
   National Institute of Standards & Technology
   Gaithersburg, MD

9. Dr. Tim Grance
   National Institute of Standards & Technology
   Gaithersburg, MD

10. Mr. Christian Grijalva
    Division Director of Defense Manpower Data Center
    Seaside, CA

11. Rob Vietmeyer, DoD CIO Cloud Lead
OSD DoD CIO
Washington, DC

12. Ron Kelly, DoD CIO ES&I Deputy
OSD DoD CIO
Washington, DC

13. Tony Simon, DoD CIO ES&I IdAM
OSD DoD CIO
Washington, DC

14. Paul Grant, DoD CIO ES&I ICAM
OSD DoD CIO
Washington, DC

15. William E. Burr
National Institute of Standards and Technology
Gaithersburg, MD

16. Donna F. Dodson
National Institute of Standards and Technology
Gaithersburg, MD

17. W. Timothy Polk
National Institute of Standards and Technology
Gaithersburg, MD

18. Jeffrey M.Voas
National Institute of Standards and Technology
Gaithersburg, MD

19. Mary Lynne Nielsen
IEEE Standards Association
Piscataway, NJ

20. Kathy L.Grise
IEEE Technical Activities
Piscataway, NJ